

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 2 8 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 5 3 1 4 5
Application Number:

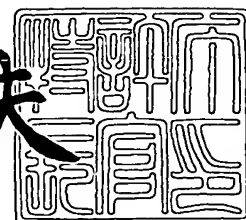
[ST. 10/C] : [J P 2 0 0 3 - 0 5 3 1 4 5]

出 願 人 東芝テック株式会社
Applicant(s): 株式会社東芝

2 0 0 4 年 2 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 1 0 7 9 1 4

【書類名】 特許願

【整理番号】 TEC067

【提出日】 平成15年 2月28日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 3/12

【発明者】

 【住所又は居所】 静岡県三島市南町 6 番 7 8 号 東芝テック株式会社 三島事業所内

 【氏名】 光富 俊之

【特許出願人】

 【識別番号】 000003562

 【氏名又は名称】 東芝テック株式会社

【代理人】

 【識別番号】 100090620

 【弁理士】

 【氏名又は名称】 工藤 宣幸

【選任した代理人】

 【識別番号】 100092576

 【弁理士】

 【氏名又は名称】 鎌田 久男

【手数料の表示】

 【予納台帳番号】 013664

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0107421

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像形成装置及び暗号キー設定入力方法

【特許請求の範囲】

【請求項 1】 入力された画像データに基づいて画像形成する画像形成装置において、

暗号キーの設定時に、ユーザにより入力された暗号キーのキー値を取り込む入力手段と、

ユーザにより予め定められた所定回数入力されたキー値が、それぞれ同一であるか否かの判断をするキー値判断手段と、

上記キー値判断手段が同一であると判断した場合に、上記入力されたキー値を暗号キーとして記憶する不揮発性記憶手段と、

入力された画像データを画像蓄積手段に蓄積する際に、その画像データに対して上記暗号キーを使用して暗号化すると共に、上記画像蓄積手段に蓄積されている暗号化された画像データを読み出す際は、上記暗号化された画像データを復元する暗号化・復元手段と

を備えることを特徴とする画像形成装置。

【請求項 2】 上記入力手段が取り込んだ上記キー値を表示すると共に、入力済みのキー値については認識不可能な表示に変換する表示手段を備える請求項 1 に記載の画像形成装置。

【請求項 3】 上記表示手段は、M桁のキー値をN ($M > N$) 桁毎に分割した場合において、あるN桁のキー値部分の入力が終わると、そのN桁のキー値部分を認識不可能な表示に変換することを特徴とする請求項 2 に記載の画像形成装置。

【請求項 4】 上記キー値の入力、表示を10進又は16進表示法に従った桁表記で行なうことを特徴とする請求項 1～3 のいずれかに記載の画像形成装置。

【請求項 5】 入力された画像データを画像蓄積手段に蓄積する際に、その画像データの暗号化に使用する暗号キーを設定入力する暗号キーの設定入力方法

であって、

ユーザにより入力された暗号キーのキー値を入力手段が取り込み、

キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、

上記キー値判断手段が同一であると判断した場合に、上記入力されたキー値を暗号キーとして不揮発性記憶手段に記憶する

ことを特徴とする暗号キー設定入力方法。

【請求項 6】 上記入力手段が取り込んだ上記キー値を表示手段が表示すると共に、入力済みのキー値については認識不可能な表示に変換することを特徴とする請求項 5 に記載の暗号キー設定入力方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、画像形成装置及び暗号キー設定入力方法に関し、入力したデータを蓄積する蓄積手段を有する画像形成装置に適用しうる。

【 0 0 0 2 】

【従来の技術】

従来、画像形成装置（例えば、複写機、ファクシミリ、プリンタ、スキャナ、複合機等）は、入力したデータを装置内の大容量蓄積装置（HDD）に蓄積し、蓄積装置から蓄積データを取り出し、その蓄積データに基づいて用紙等に複写して出力する。

【 0 0 0 3 】

そのため、蓄積装置には入力したデータそのものが蓄積されており、例えば、蓄積手段を盗み出した後に、他の装置等を駆使して蓄積されているデータが悪意に取り出され、情報が流出してしまうという情報漏洩の問題がある。特に、機密文書についての機密文書の漏洩が問題とされる。

【 0 0 0 4 】

従来、このような問題を解決するために、次のような手段を行なうことにより機密文書の漏洩を防止していた。

【0005】

まず、最初の機密文書漏洩防止手段は、例えば、特定の機密文書について、複写機による複写を禁止することで、機密文書の漏洩を防止していた。

【0006】

次に、また例えば、複写機による文書の複写を許可複写機による文書の複写を行なう場合、複写を許可されたユーザにのみパスワード等を付与して、そのパスワード等に基づいてユーザ認証を行なうことにより、許可されたユーザ以外の者による複写により、複写機内に蓄積された画像情報をアクセスできないようにして、情報の漏洩を防止していた。

【0007】

そして、下記の特許文献1及び2は、パスワード等の設定入力方法について記載されている。

【0008】**【特許文献1】**

特開2001-166843号公報

【0009】**【特許文献2】**

特開平10-63621号公報

【0010】**【発明が解決しようとする課題】**

しかしながら、上述した機密文書漏洩防止手段によると、それぞれ次のような問題がある。

【0011】

上述した最初の機密文書漏洩防止手段の場合、特定の機密文書の複写を禁止することにより、社内の人間の手による機密文書の複製品が、社外に漏洩することを防げるが、社内での使用においては、複写機の本来の機能を制限することになり、利便性を損なう。

【0012】

また、次の機密文書漏洩防止手段は、パスワード等を使用するユーザ認証につ

いては、複写機が通電中は、ユーザ認証プログラムが動作しているため、不正アクセスを防止できるが、複写機が電源オフ中に、内部の蓄積装置（HDD）のみ取り外して、他の装置（例えばパソコン）に、そのHDDを接続して、内部情報の解析をされた場合、認証プログラムが効かないため、内部情報は容易に解読される可能性がある。

【0013】

ところで、例えばファクシミリ等のネットワークを利用する情報通信の分野において、情報通信を行なう場合、伝送路上での情報の漏洩を防ぐため、情報を暗号化して送信することが行われており、この暗号化方式を入力した画像データにも適用し、蓄積装置に書込む画像データをすべて暗号化してから書込むことで蓄積装置が盗まれても、書込まれた画像データが解読できないようにすることができる。

【0014】

一般的に利用されている暗号化方式は、予め設定された暗号キーを使用するため、蓄積装置内のデータが解読されないためにも、暗号キーも第三者に知られることなく、かつ、どこに暗号キーを格納しているかをも知られないようにすることが望ましい。

【0015】

しかし、暗号キーの初期設定時や、既に設定登録済みの暗号キーが何らかの原因により消失等した場合には、改めて暗号キーを設定入力する必要がある、この場合には、暗号キーのキー値を正しく入力することが必要となる。間違えて再設定してしまった場合には、既に蓄積されているデータの読み出しが不可能になったり、暗号化処理が正しく行なわれない場合もある。

【0016】

そのため、入力画像データを蓄積装置に蓄積する際に、暗号化したデータを蓄積する画像形成装置において、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定が正しく行なえ得る暗号キー設定入力方法と、その画像形成装置が求められている。

【0017】

【課題を解決するための手段】

かかる課題を解決するために、第1の本発明の画像形成装置は、入力された画像データに基づいて画像形成する画像形成装置において、暗号キーの設定時に、ユーザにより入力された暗号キーのキー値を取り込む入力手段と、ユーザにより予め定められた所定回数入力されたキー値が、それぞれ同一であるか否かの判断をするキー値判断手段と、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして記憶する不揮発性記憶手段と、入力された画像データを画像蓄積手段に蓄積する際に、その画像データに対して暗号キーを使用し暗号化すると共に、画像蓄積手段に蓄積されている暗号化された画像データを読み出す際は、暗号化された画像データを復元する暗号化・復元手段とを備えることを特徴とする。

【0018】

また、第2の本発明の暗号キー設定入力方法は、入力された画像データを画像蓄積手段に蓄積する際に、その画像データの暗号化に使用する暗号キーを設定入力する暗号キーの設定入力方法であって、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することを特徴とする。

【0019】**【発明の実施の形態】****(A) 第1の実施形態**

以下では、本発明の画像形成装置の第1の実施形態について図面を参照して説明する。

【0020】

なお、本実施形態は、画像形成装置の一例としてデジタル複写装置（DPPC）を例に挙げて説明するが、入力された画像を蓄積する蓄積手段を有する画像形成装置（例えば、プリンタ、ファクシミリ、複合機等）に広く適用できる。

【0021】

本実施形態は、入力した画像データを機体個別の暗号キーを使用して暗号化した画像データを大容量蓄積装置（HDD）に蓄積する場合であって、初期設定時、又は、何らかの事情により機体個別の暗号キーが消失した時に、ユーザにより、その機体個別の暗号キーを不揮発性メモリ（NVRAM）に設定入力させる方法について説明する。

【0022】

（A-1）第1の実施形態の構成

図1は、本実施形態に係るデジタル複写装置の構成ブロックの概略を示すものである。

【0023】

図1に示すように、本実施形態に係る画像形成装置は、装置全体を制御するシステム制御部1と、原稿をデジタル信号に変換してデジタル信号の画像データを出力するスキャナサブシステム2と、デジタル信号の画像データに基づいて画像を用紙に印刷して出力するプリンタサブシステム4と、用紙ジャム等の画像形成装置の状態を表示したり、ユーザが複写を行うときの各種パラメータや動作モードを入力する制御パネル7とを備えるものである。

【0024】

スキャナサブシステム2、プリンタサブシステム4及び制御パネル7は、それぞれCPU203、43及び74を搭載しており、これらCPU203、43及び74は、全体の制御を行うシステム制御部1のシステムCPU10とそれぞれシリアルIFを介して制御情報を送受信し各ブロックの制御を行なう。

【0025】

システム制御部1は、図1に示すように、システム制御回路5と、複数の画像データを蓄積できるHDDブロック80との2つの基板構成を有するものである。

【0026】

HDDブロック80は、大容量蓄積装置（以下HDDと呼ぶ）830と、暗号復元化回路810と、暗号キーメモリ820と、IDEコントローラ800とを有するものである。

【0 0 2 7】

HDD 8 3 0 は、暗号化回路 8 1 0 により暗号化された複数の画像データを蓄積するものである。HDD 8 3 0 に暗号化した画像データを蓄積する場合の例として、例えば、本実施形態の画像形成装置の場合、複数枚のコピーを行なう際に、画像データを暗号化して HDD 8 3 0 に記憶し、その蓄積した画像データに基づいて複数枚のコピーを実行する場合や、両面コピーを行なう際に、暗号化した画像データを HDD 8 3 0 に記憶し、その蓄積した画像データに基づいて両面コピーを実行する場合や、又用紙の片面につき 2 ページ文の画像を並べて印刷する 2 i n 1 印刷を実行する場合などがある。

【0 0 2 8】

暗号・復元化回路 8 1 0 は、画像データの暗号化処理の際、I D E コントローラ 8 0 0 を介してページメモリ制御回路 3 0 によって圧縮処理が行なわれた画像データを受け取り、その圧縮された画像データを暗号キーに基づいて暗号化して、暗号化した画像データを HDD 8 3 0 に蓄積するものである。また、暗号・復元化回路 8 1 0 は、暗号化された画像データの復元処理の際、HDD 8 3 0 に蓄積されている暗号化された画像データを読み出し、その暗号化された画像データを暗号キーに基づいて復元して、復元した画像データ（すなわち、元の圧縮された画像データ）を I D E コントローラに与えるものである。

【0 0 2 9】

ここで、暗号・復元化回路 8 1 0 が行なう暗号・復元化方式は、機体個別の暗号キーを使用して、元のデータを解読不可能な別のデータに変形し、又その暗号キーを使用して、暗号化したデータを元のデータに復元する暗号・復元化方式であれば広く適用できる。この機体個別の暗号キーは、装置製造の際にそれぞれの装置毎に設定された暗号キーである。

【0 0 3 0】

暗号キーメモリ 8 2 0 は、画像データの暗号化及び復元に使用する暗号キーを記憶する揮発性のメモリである。暗号キーメモリ 8 2 0 は、暗号・復元化回路 8 1 0 による画像データの暗号化及び復元処理の際に、N V R A M 1 4 に記憶されている暗号キーを受け取り、電源オン中は暗号キーを記憶し、電源がオフになる

と、その暗号キーを廃棄する記憶手段である。

【0031】

IDEコントローラ800は、システムバス9と、HDD830と、暗号化回路810と、暗号キーメモリ820と、システムバス9とのインタフェースである。IDEコントローラ800は、システムバス9を介して、ページメモリ制御回路30から圧縮処理された画像データを受け取り、暗号・復元化回路810に与えるものである。また、IDEコントローラ800は、暗号・復元化回路810により復元された画像データを、システムバス9を介して、ページ制御回路30に与えるものである。

【0032】

次に、システム制御回路5の内部構成について説明する。

【0033】

システム制御回路5は、システムCPU10と、メインメモリ12と、ROM11と、NVRAM14と、ページメモリ制御回路30と、LANコントローラ60とを有するものである。

【0034】

なお、システムCPU10と、メインメモリ12と、ROM11と、NVRAM14とは、ローカルバス15を介して接続されている。また、システムCPU10と、HDDブロック80と、ページメモリ制御回路30と、LANコントローラ60とは、システムバス9を介して接続されている。

【0035】

NVRAM14は、マシン毎の設定値を格納するバッテリでバックアップする不揮発性の記憶手段である。また、NVRAM14は、画像データの暗号化に使用される暗号キーを記憶しており、電源オン後、暗号・復元化回路810により暗号化又は復元する際に、その記憶している暗号キーを暗号キーメモリ820に与えるものである。

【0036】

システムCPU10は、装置全体を制御するものである。システムCPU10の詳細な内部構成については後述する。

【0037】

ROM11は、装置全体を制御する制御プログラムを記憶するものである。ROM11は、電源オン時に所定の規則に従って、システムCPU10により記憶している制御プログラムが読み出され、当該制御プログラムによりブート処理がなされる。また、ROM11は、本実施形態の暗号キーの設定入力に係るプログラムも記憶する。

【0038】

メインメモリ12は、揮発性のDRAMで構成されており、電源オン時に、システムCPU10がROM11からロードした制御プログラムを、所定の領域に記憶するものである。また、メインメモリ12は、電源オン中に、記憶した制御プログラムを動作するものである。また、メインメモリ12は、ユーザにより入力された暗号キー設定に係るキー値を一時的に記憶するものである。

【0039】

本実施形態では、暗号キー設定に係るキー値を複数回（例えば2回）ユーザに入力してもらい、それらキー値が共に正しい場合には、そのキー値を暗号キーとする。

【0040】

ページメモリ制御回路30は、画像データ（デジタル信号）を一時的にページ単位で記憶するものである。ページメモリ制御回路30は、画像データをページ毎に一時的に記憶するページメモリ300と、このページメモリ300を制御するページメモリ制御部301とを有する。また、ページメモリ制御回路30は、要求に応じて、画像データの圧縮処理及び圧縮された画像データの伸長処理が行なうものである。

【0041】

LANコントローラ60は、図示しないネットワーク上に接続された端末（例えば、パソコン等）と画像形成記憶装置との間での、画像データの送受信をインタフェースするものである。

【0042】

制御パネル7は、マシンの状態を表示したり又は各種パラメータの情報を表示

するLCD70と、LCD70上に配置されるタッチパネル71と、テンキー（Key）72と、複数のLED部73と、これら制御パネル7の各構成を制御するパネルCPU74とを有するものである。

【0043】

本実施形態では、入力手段として、タッチパネル71及びKey72を備えるものとしたが、ユーザにより入力操作し得る入力手段であれば広く適用できる。

【0044】

タッチパネル71及びKey72の入力手段は、初期設定の場合又は何らかの事情により暗号キーがNVRAM14から消失した場合等に、ユーザが入力した暗号キーのキー値を取り込むものである。この暗号キーが正しいものであるか否かの判断は、暗号キーのキー値を2回以上（本実施形態では2回とする）ユーザに入力してもらい、その1回目のキー値と2回目のキー値との同一性を判断することによる。そして、1回目と2回目とのキー値が同一であれば、そのキー値を暗号キーとし、1回目と2回目とのキー値が異なっていれば、そのキー値に基づく暗号キーを設定せずエラーとする。

【0045】

LCD70は、ユーザが入力した暗号キーのキー値を表示する表示部である。LCD70は、ユーザにより入力されたキー値を4桁ごとに区切って、その4桁キー値の入力が終了すると、表示していたキー値をアスタリスク「*」に変換して表示する。これを一般的に表現すると、例えばM桁（Mは1以上の整数）のキー値をN桁（Mは1以上の整数）（ $M > N$ ）毎に分割した場合において、あるN桁のキー値部分の入力が終わると、そのN桁のキー値の部分をアスタリスク「*」に変換表示するということになる。これは、LCD70に表示されたキー値が第三者に盗み見られることを防止するためである。

【0046】

また、本実施形態ではキー値をアスタリスク「*」表示に変換することとするが、アスタリスクに限ることなく、入力したキー値を認識不可能な表示に変換できれば、例えば「-」や「#」や「スペース（空白）」などの表示であってもよい。

【0047】

次に、上述したシステム制御回路5のシステムCPU10の内部構成について説明する。図2は、システムCPU10の内部構成ブロック図を示したものである。

【0048】

図2に示すように、システムCPU10は、ROM11の制御プログラムを実行するCPUコア100と、ローカルバス15上のメインメモリ12（SDRAM）の制御を行うDRAMコントローラ101と、同じくローカルバス15上のROM11及びNVRAM14を制御するROMコントローラ102と、ローカルバス15とSDRAMコントローラ101とROMコントローラ102とをインタフェースするローカルバスI/F103と、装置上の各ブロックから割り込みを入力し、所定の優先度順位に基づいて唯一の割り込みをCPUコア100に通知する割り込みコントローラ104と、スキャナCPU203とプリンタCPU43と制御パネルCPU74とCPUコア100とが通信するためのインタフェースをする3チャンネルのシリアルI/O（SIO）105と、システムバス9上の各ブロックとシステム制御部1上の各ブロックとをインタフェースするシステムバスコントローラ106と、タイマー107と、CPUコア100とこれらシステムCPU10の各ブロック（DRAMコントローラ101、ROMコントローラ102、割り込みコントローラ104、3チャンネルのシリアルI/O（SIO）105、システムバスコントローラ106、タイマー107）とを接続する内部バス108とを有するものである。

【0049】

次に、上述したページメモリ制御回路30のページメモリ制御部301の内部構成について説明する。図3は、ページメモリ制御部301の内部構成を示すものである。

【0050】

図3に示すように、ページメモリ制御部301は、内部の各ブロックとシステムバス9とのインタフェースを行うシステムバスインタフェース（システムバスIF）32と、LCDコントローラ33と、LEDコントローラ34と、ページ

メモリ 300 を制御し、かつ、ページメモリ 300 とシステムバス 9 上の後述するデバイスとスキャナ画像 I F 9 2 を介して接続されたスキャナサブユニット 2 とプリンタ画像 I F 9 1 を介して接続されたプリンタサブユニット 4 との間で画像データの転送を制御する PM-CON 3 5 を有するものである。

【0051】

PM-CON 3 5 は、ページメモリ 300 をアクセスするデバイスからのアクセス要求を所定の優先度順位で調停し、順次アクセス要求に基づいてページメモリ 300 をアクセスする。

【0052】

このページメモリ 300 をアクセスするデバイスとしては、スキャナ画像 I F 9 2 を介して画像データをページメモリ 300 へ書き込むスキャナイメージプロセッシング部 202、プリンタ画像 I F 9 1 を介してページメモリ 300 上の画像データを読み出すプリンタイメージプロセッシング部 41、システム CPU 10、LCD コントローラ 33、ページメモリ 300 上の画像データを HDD 830 へ蓄積したり又は HDD 830 に蓄積された画像データをページメモリ 300 へ戻したりする IDE コントローラ 800 がある。

【0053】

また、ページメモリ 300 は、画像データを一時的に記憶する領域の他に、LCD 70 に表示するための表示データを記憶する表示データ領域が設けられており、LCD コントローラ 33 は、周期的に表示データ領域に記憶されている表示データを読み出し、制御パネル 7 上の LCD 70 が出力する同期信号に同期して、表示データを LCD 70 へ出力する。LCD 70 は、表示データを順次表示する。

【0054】

次に、ページメモリ 300 の PM-COM 3 5 の内部構成について説明する。
図 4 は、PM-COM 3 5 の内部構成を示した構成図である。

【0055】

PM-COM 3 5 は、ページメモリ 300 と他の処理ブロックとのデータ転送をインタフェースする転送チャンネルと、データ処理ブロック（圧縮処理 3530

及び伸長処理 3531) と、回転処理 3532 と、各転送チャンネル毎にページメモリ 30 のアドレスを発生するアドレス発生部と、PDRAM 制御部 36 とを有するものである。

【0056】

転送チャンネルは、スキャナ IF 3501 と、プリンタ IF 3509 と、HDD 転送 (ch0) 3504 と、HDD (ch1) 3506 と、圧縮 (入力) 3502 と、圧縮 (出力) 3503 と、伸長 (入力) 3507 と、伸長 (出力) 3508 と、メモリクリア 3510 と、CPU IF 3511 と、LCD IF 3512 とを有する。

【0057】

また、アドレス発生部は、AGC (ch0) 3520 と、AGC (ch1) 3521 と、AGC (ch2) 3522 と、AGC (ch3) 3523 と、AGC (ch4) 3524 と、AGC (ch5) 3525 と、FIFO (ch1-A) 3526 と、FIFO (ch1-B) 3527 と、FIFO (ch0-A) 3528 と、FIFO (ch0-B) 3529 とを有する。

【0058】

図 1 に戻り、スキャナサブシステム 2 は、少なくとも、原稿を所定のタイミングで搬送する図示しない原稿搬送部と、原稿搬送に同期して、原稿をライン単位で、光学的に読み取り電気信号に変換する CCD 201 と、CCD 201 が出力する電気信号を所定の画素 (例えば 8 bit/画素) に変換し、文字モード、文字写真モード、写真モード等指定された画像モードに適した画像処理を実行した後、1 bit/画素のデータに階調処理し、所定のタイミングで画像データをスキャナ画像 IF 92 を介して、ページメモリ制御部 3 へ出力するスキャナイメージプロセッシング部 202 と、スキャナサブユニット 2 を制御するスキャナ CPU 203 等を有するものである。

【0059】

プリンタサブシステム 4 は、少なくとも、ページメモリ 300 に一時的に記憶された画像データを、プリンタ画像 IF 91 を介して、所定のタイミングで読み出し、指定されたモードで画像処理するプリンタイメージプロセッシング部 41

と、プリンタイメージプロセッシング部 41 からの画像データを光信号に変換するレーザドライブ回路 42 と、レーザドライブ回路 42 の光信号に基づいて、静電記録方式により、像を形成し、所定の用紙に転写して出力する図示しない像形成部と、プリンタサブシステム 4 を制御するプリンタ CPU 43 等を有するものである。

【0060】

(A-2) 第 1 の実施形態の動作

以下では、第 1 の実施形態の画像形成装置において、画像データを暗号化に使用する暗号キーの設定入力方法の動作について図面を参照して説明する。

【0061】

図 5 は、本実施形態に係る暗号キーの設定を説明するフローチャートである。

【0062】

本実施形態の画像形成装置の画像データの暗号化に使用する機体個別の暗号キーを初期設定又は何らかの事情により暗号キーが消失した場合に、ユーザにその暗号キーのキー値の入力要求を求めるよう、LCD 70 に表示する。勿論、LCD 70 に暗号キーのキー値の入力要求の表示させることなく、ユーザの操作により設定入力を開始させるようにしてもよい。

【0063】

タッチパネル 71 又は Key 7 を介して、ユーザにより暗号キーのキー値が入力される。(S1)。

【0064】

ここで、本実施形態では、暗号キーのキー値を 16 進数表示の 16 桁 (64 bit) で表示したものとする。なお、この暗号キーのキー値に所定ビット数の誤り検出符号を設けるようにしてもよい。

【0065】

LCD 79 には、ユーザにより入力された暗号キーのキー値が表示される (S2)。図 6 は、入力される暗号キーのキー値の表示イメージを示す。

【0066】

図 6 (A) に示すように、ユーザが入力するキー値は、4 桁毎に表示する。図

6 (B) に示すように、ユーザが4桁のキー値が入力され、次の桁のキー値(4の倍数の次の桁のキー値)が入力されると、既に入力された前の4桁のキー値が、アスタリスク「*」に変換された形で表示される。または、4桁のキー値の入力が終わった時点で、その4桁のキー値をアスタリスクに変形してもよい。

【0067】

これを繰り返し、図6 (C) のように、16桁のすべてのキー値が入力されると、図6 (D) に示すように、16桁すべてのキー値がアスタリスク「*」に変換されて表示される(S3)。

【0068】

次に、ユーザがS1～S3で入力したキー値を再度入力要求をする。このとき、第1回目と同様に、4桁ずつのキー値を表示し、4桁のキー値の入力が終了し次の桁のキー値が入力されると、その前の4桁のキー値をアスタリスク「*」に変換表示する(S4～S6)。

【0069】

第1回目に入力されたキー値と、第2回目に入力されたキー値とが同一であるか否かが判断される(S7)。

【0070】

その結果、第1回目と第2回目とも同一のキー値である場合には、そのキー値が暗号キーとしてNVRAM14に設定される(S8)。

【0071】

また、第1回目に入力されたキー値と、第2回目に入力されたキー値とが異なる場合には、暗号キーとして入力されたキー値に誤りがあったとして設定されない。この場合、再度ユーザに暗号キーのキー値入力を要求してもよい。

【0072】

以上のようにして、初期設定時又は暗号キーの消失などの場合に、ユーザにより暗号キーを設定入力させることができる。

【0073】

(A) 第1の実施形態の効果

以上、第1の実施形態によれば、初期設定時又は何らかの事情により画像デー

タの暗号化に使用する暗号キーを、暗号化画像データを蓄積するHDD830とは別の基板からなる不揮発性メモリ（NVRAM14）に記憶することにより、HDD830が盗まれたとしても、NVRAM14が無事であれば、HDD830の蓄積データの解読を防止することができる。

【0074】

また、第1の実施形態によれば、ユーザによる暗号キーの設定入力を複数回行なわせ、その複数回入力された暗号キーがすべて同一のものであるか否かを判断することにより、セキュリティを高めることができる。

【0075】

更に、第1の実施形態によれば、ユーザにより入力させた暗号キーを所定の桁数毎にアスタリスクに変換表示することにより、第三者による盗み見を防止することができる。

【0076】

（B）他の実施形態

（B-1）上述した実施形態は、デジタル複写装置に適用した場合について説明したが、データを暗号化し、その暗号化したデータを蓄積する蓄積装置（HDD）を有する画像形成装置（例えばプリンタ、ファクシミリ、複合機等）に広く適用できる。

【0077】

例えば、画像形成装置がプリンタである場合、例えば、プリンタは、ユーザが使用する端末装置（例えばパソコン等）から取り入れた画像データを受け取り、複数の用紙にプリントするような場合に、画像データを暗号化してHDDに記憶してプリントする場合に適用できる。

【0078】

また例えば、画像形成装置がファクシミリである場合、例えば、ファクシミリは、伝送されてきた情報の受信時や、送信メモリ時等に適用できる。

【0079】

（B-2）また、画像形成装置が複合機（例えば複写機能とプリンタ機能とファクシミリ機能とを有する複合機）である場合、各機能モード毎に異なる暗号キー

を設定して使用するようにしてもよい。

【0080】

(B-3) 上述した第1の実施形態では、ユーザに入力されたキー値を4桁毎に表示し、次の桁のキー値が入力された後にその入力された4桁のキー値をアスタリスクに変換して表示することとしたが、これに限ることなく、第三者による盗み見を防止できれば、例えば、1桁のキー値が入力される毎や、又は8桁のキー値入力毎等のように適用することができる。

【0081】

(B-4) 上述した第1の実施形態では、第1回目に入力されたキー値と第2回目のキー値とが同一か否かの判断は、第2回目のキー値が入力された後に行なうこととして説明したが、これに限らず、例えば、1桁のキー値の入力毎や、又4桁毎のキー値の入力毎に同一性の判断をするようにしてもよい。

【0082】

(B-5) 上述した第1の実施形態において、暗号キーを機体個別の暗号キーであり、初期設定時又は何らかの事情により暗号キーが消失した場合に、新たに設定入力する暗号キーも、その機体個別の暗号キーであるとして説明したが、この新たに設定入力する暗号キーをユーザ独自に決定した暗号キーを適用するようにしてもよい。

【0083】

(B-6) 上述した第1の実施形態において、LCD70は、前回設定入力した暗号キーのキー値を表示するようにしてもよい。

【0084】

また、上述した第1の実施形態では、キー値の入力、表示を16進表示として説明したが、10進表示法に従った桁表記で行なうようにしてもよい。

【0085】

【発明の効果】

以上、第1及び第2の本発明によれば、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であ

ると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することにより、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定入力が正しく行なえることができる。

【図面の簡単な説明】

【図 1】 第1の実施形態の画像形成装置の全体構成ブロックを示したものである。

【図 2】 第1の実施形態のシステム CPU 10 の内部構成を示したブロック図である。

【図 3】 第1の実施形態のページメモリ制御部 301 の内部構成を示したブロック図である。

【図 4】 第1の実施形態の PM-COM 35 の内部構成を示した簿六層である。

【図 5】 第1の実施形態の暗号キーの設定入力動作のフローチャートである。

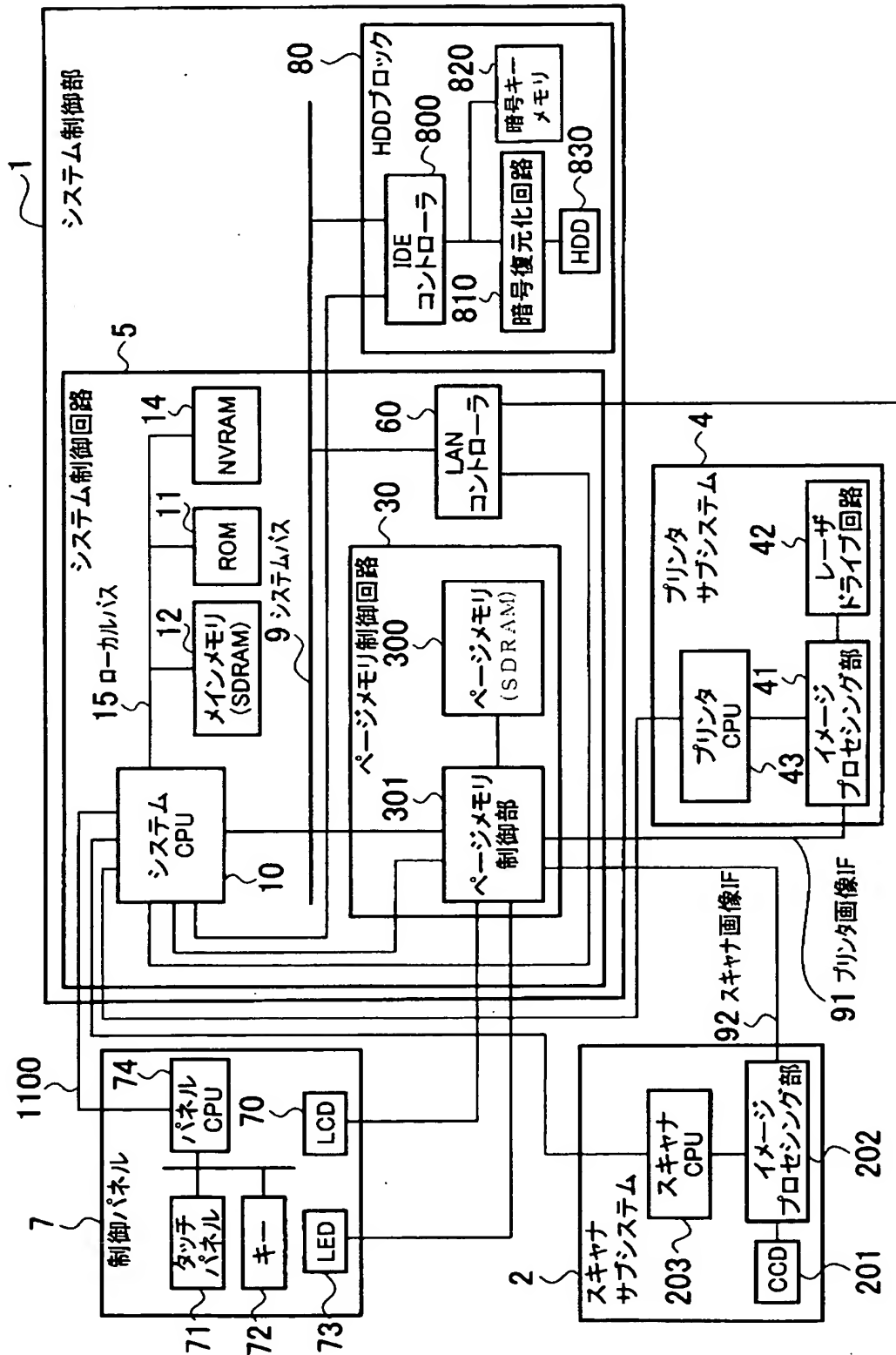
【図 6】 入力される暗号キーの表示イメージを説明する説明図である。

【符号の説明】

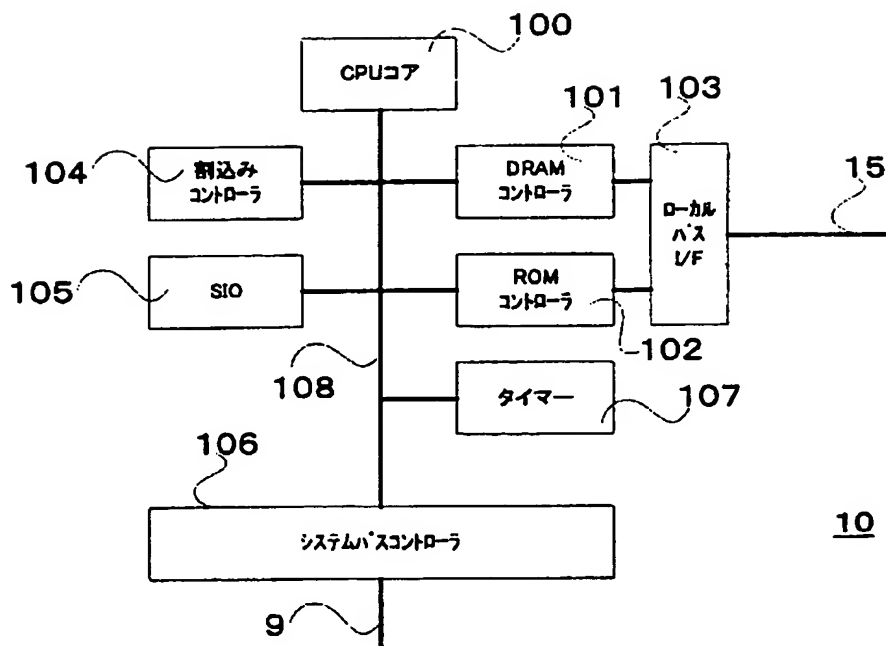
7…制御パネル、70…LCD、71…タッチパネル、72…キー、
74…パネルCPU、14…NVRAM、80…HDDブロック、
810…暗号復元化回路、830…HDD、800…IDEコントローラ。

【書類名】 図面

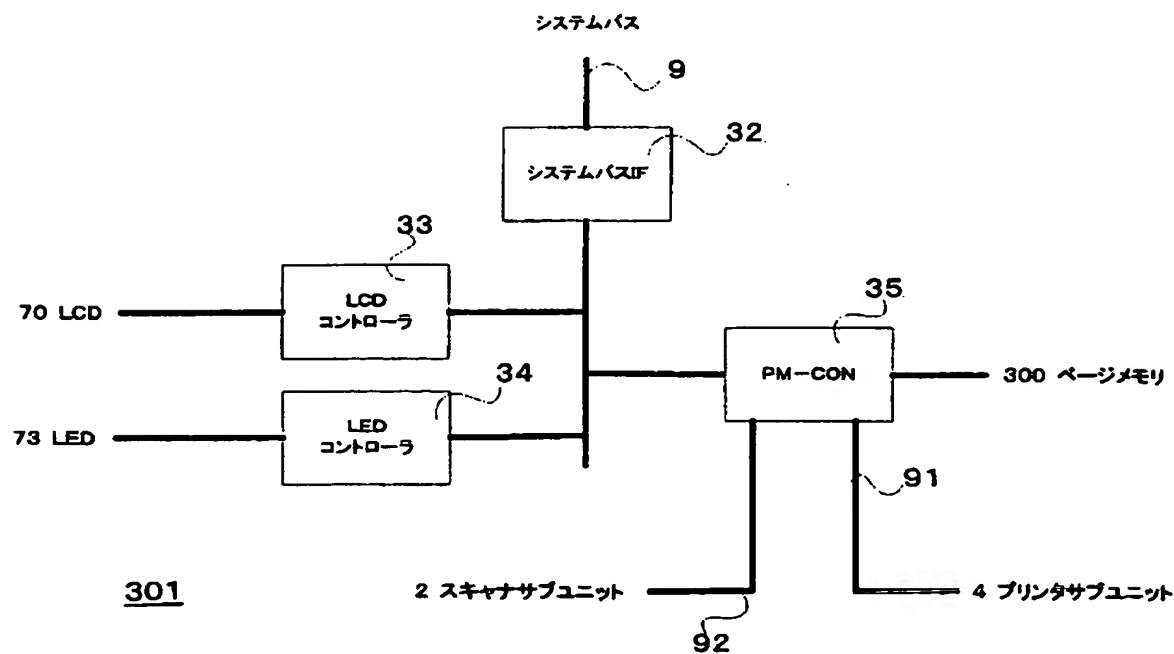
【図 1】



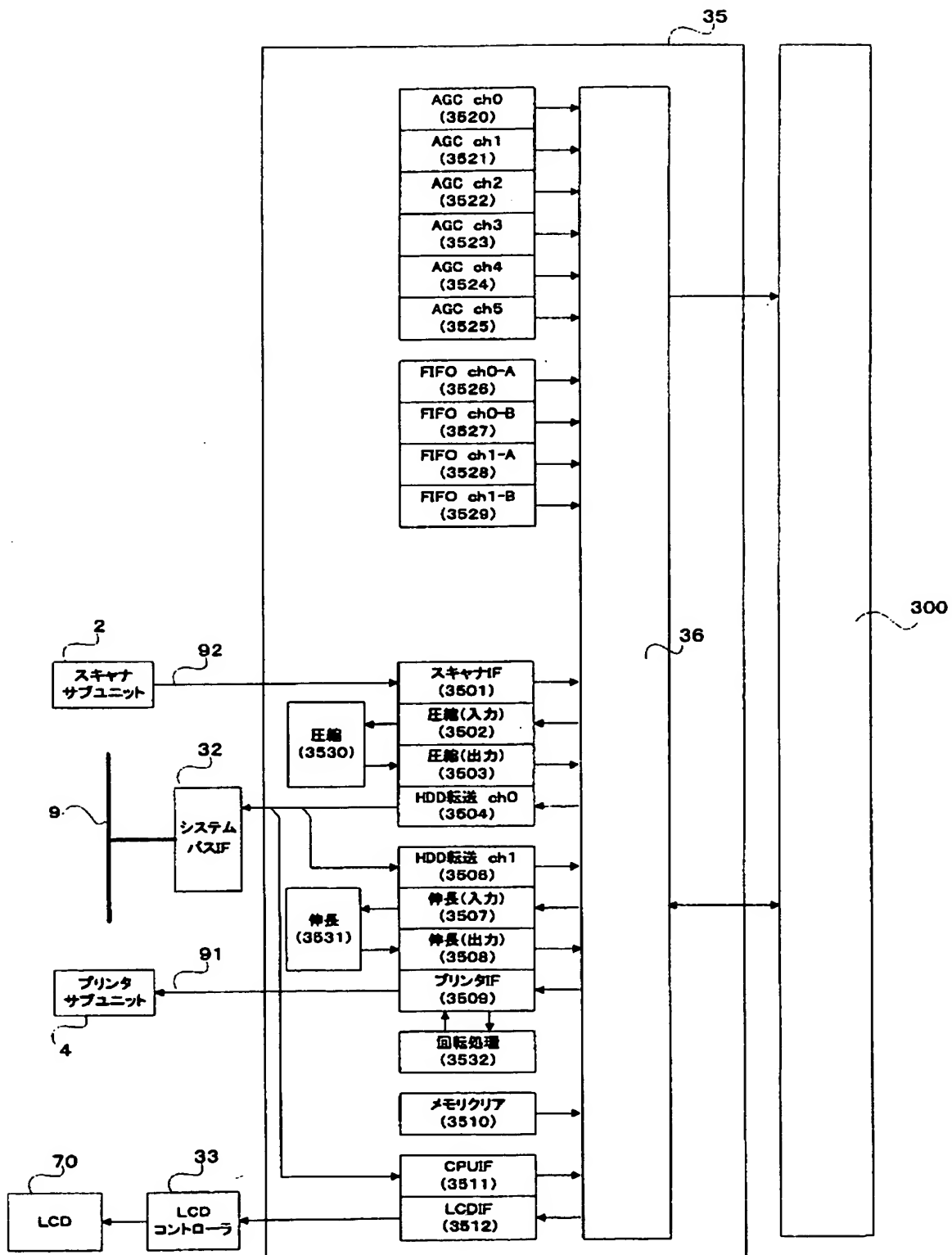
【図 2】



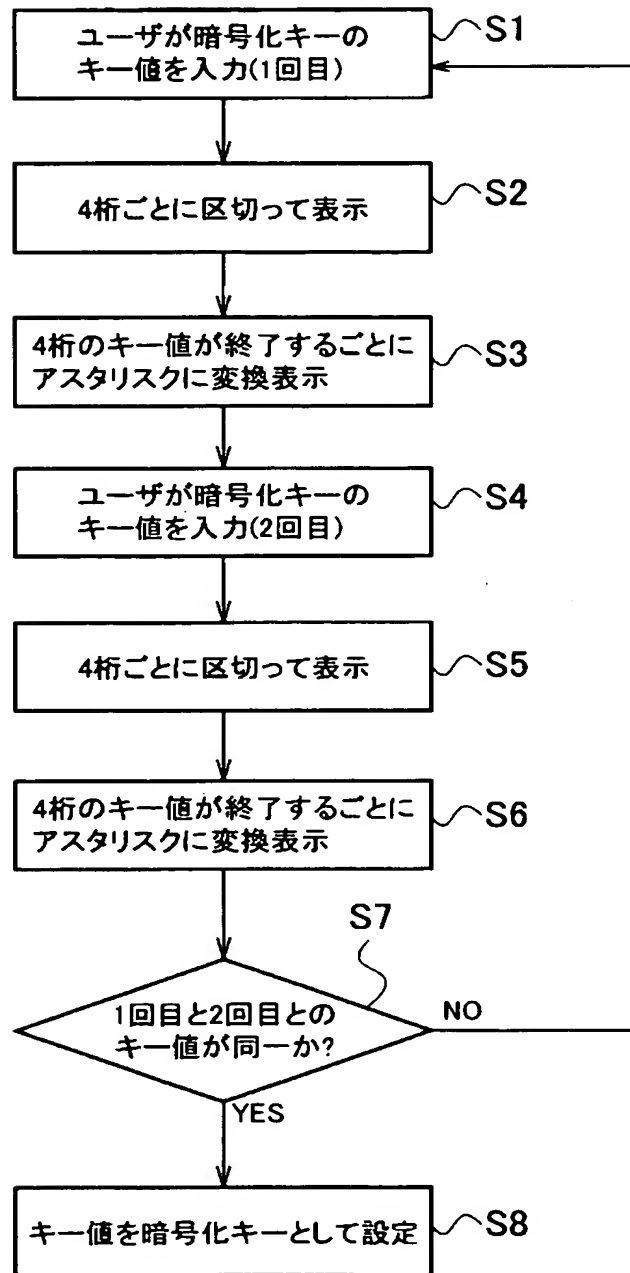
【図 3】



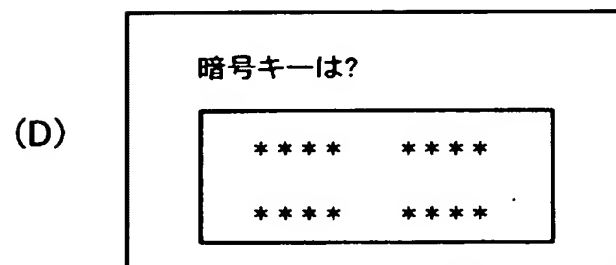
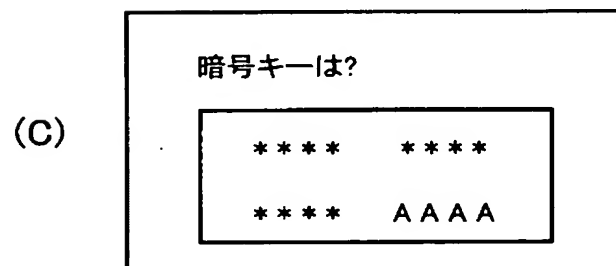
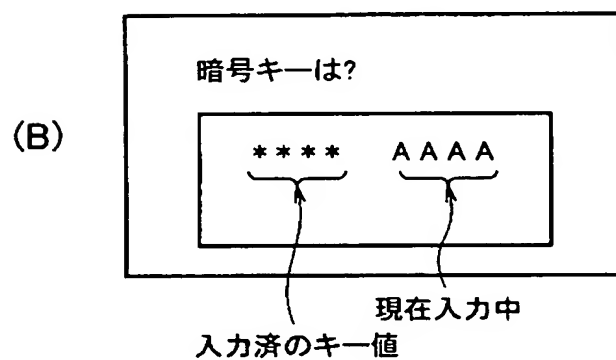
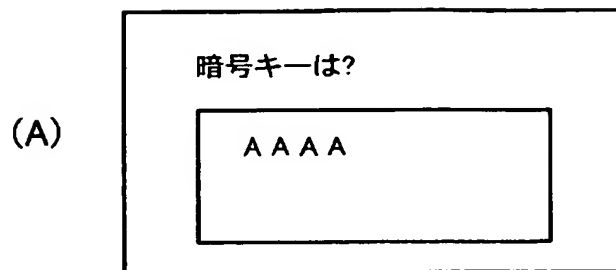
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 入力画像データを暗号化して蓄積する際に、暗号化に供する暗号キーの設定入力時に、ユーザにより暗号キーの設定が正しく行なえ得る暗号キー設定入力方法と、画像形成装置とを提供する。

【解決手段】 本発明の暗号キー設定入力方法は、ユーザにより入力された暗号キーのキー値を入力手段が取り込み、キー値判断手段がユーザにより予め設定された所定回数入力されたキー値が同一であるか否かの判断し、キー値判断手段が同一であると判断した場合に、入力されたキー値を暗号キーとして不揮発性記憶手段に記憶することを特徴とする。

【選択図】 図 1

【書類名】 出願人名義変更届
【整理番号】 TEC067M
【提出日】 平成15年12月 4日
【あて先】 特許庁長官 今井 康夫 殿
【事件の表示】
 【出願番号】 特願2003- 53145
【承継人】
 【識別番号】 000003078
 【氏名又は名称】 株式会社東芝
 【代表者】 岡村 正
【承継人代理人】
 【識別番号】 100090620
 【弁理士】
 【氏名又は名称】 工藤 宣幸
 【電話番号】 03(3981)8899
【手数料の表示】
 【予納台帳番号】 013664
 【納付金額】 4,200円
【提出物件の目録】
 【物件名】 一部譲渡証書 1
 【提出物件の特記事項】 手続補足書により提出する
 【物件名】 株式会社東芝の委任状 1
 【提出物件の特記事項】 手続補足書により提出する
 【包括委任状番号】 0107421

認定・付加情報

特許出願の番号	特願 2003-053145
受付番号	50302001592
書類名	出願人名義変更届
担当官	伊藤 雅美 2132
作成日	平成16年 1月19日

<認定情報・付加情報>

【承継人】

【識別番号】	000003078
【住所又は居所】	東京都港区芝浦一丁目1番1号
【氏名又は名称】	株式会社東芝

【承継人代理人】

申請人	
【識別番号】	100090620
【住所又は居所】	東京都豊島区南池袋2丁目41番8号 池袋睦ビル2階 工藤特許事務所
【氏名又は名称】	工藤 宣幸

特願 2 0 0 3 - 0 5 3 1 4 5

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 3 5 6 2]

1. 変更年月日 1 9 9 9 年 1 月 1 4 日

[変更理由] 名称変更

住所変更

住 所 東京都千代田区神田錦町 1 丁目 1 番地
氏 名 東芝テック株式会社

特願 2 0 0 3 - 0 5 3 1 4 5

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 3 0 7 8]

1. 変更年月日	2 0 0 1 年 7 月 2 日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目 1 番 1 号
氏 名	株式会社東芝